REMARKS

In the Office Action dated September 30, 2003, the Examiner objected to the disclosure due to informalities; objected to the drawings as failing to comply with 37 C.F.R. § 1.84(p)(4); rejected claim 11 under 35 U.S.C. § 112, second paragraph as being indefinite; rejected claims 1-6, 9-11, and 17-18 under 35 U.S.C. § 102(e) as being anticipated by Dworkin et al. (U.S. Patent No. 6,230,179); rejected claim 13 under 35 U.S.C. § 103(a) as being unpatentable over Dworkin et al. in view of Carroll et al. (U.S. Patent No. 3,064,896); and rejected claims 14-15 under 35 U.S.C. § 103(a) as being unpatentable over Dworkin et al. in view of Carroll et al., and in further view of Zook (U.S. Patent No. 5,467,297). The Examiner also indicated that claim 16 would be allowable if rewritten in independent form.

By this Amendment, Applicants have overcome the objection to the disclosure and drawings; cancel claim 1, without prejudice or disclaimer of the subject matter thereof; amend claims 2, 6, 11, and 13; and add new claim 19. In view of the following remarks, Applicants respectfully traverse the Examiner's rejections of the claims under 35 U.S.C. §§ 112, 102(e), and 103(a).

With regard to the Examiner's objection to the disclosure due to informalities, Applicants herewith amended the specification in the manner suggested by the Examiner. These objections are thus overcome.

The Examiner objected to the drawings as failing to comply with 37 C.F.R. § 1.84(p)(4). Specifically, the Examiner indicated that reference characters "22" (in the drawings) and "22a" (in the specification) have both been used to designate "finite field GF(2^m) arithmetic controller." In response, Applicants amend the specification in the appropriate locations.

Additionally, the Examiner indicated that there is a spelling error in FIG. 14. Applicant herewith submits a replacement drawing sheet correcting the spelling error.

The Examiner rejected claim 11 under 35 U.S.C. § 112, second paragraph, as being indefinite. Specifically, the Examiner alleged that the claim refers to a controller, but it is unclear from the specification as to the specific function of the controller and the controller's function with regard to the claimed apparatus.

Applicants respectfully traverse this rejection. Claim 11 is supported by the specification, for example, at page 35, line 25 to page 36, line 10, and at page 38, lines 22-25. More particularly, in one exemplary embodiment, a finite field GF(2^m) arithmetic controller 22 may have a modulo function added to it. For example, in addition to the function of controlling an arithmetic unit 4 to obtain a multiply result c'(x) of equation (5), finite field GF(2^m) arithmetic controller 22 may have the function of controlling arithmetic unit 4 and quotient acquisition circuit 50 to execute a modulo for the multiply result c'(x) using a modulo polynomial f(x). In view of the foregoing, Applicants respectfully request that the rejection of claim 11 under 35 U.S.C. § 112, second paragraph, be removed.

In making the above references to the specification, it is to be understood that Applicants are in no way intending to limit the scope of the claims to the exemplary embodiments shown in the drawings and described in the specification. Rather, Applicants expressly affirm that they are entitled to have the claims interpreted broadly, to the maximum extent permitted by statute, regulation and applicable case law.

In order to properly anticipate Applicants' claimed invention under 35 U.S.C. § 102, each and every element of the claim in issue must be found, either expressly described or under principles of inherency, in a single prior art reference. Furthermore, "[t]he identical invention must be shown in as complete detail as is contained in...the claim." See M.P.E.P. § 2131 (8th Ed., Aug. 2001), quoting *Richardson v. Suzuki Motor Co.*, 868 F.2d 1126, 1236, 9 U.S.P.Q. 2d 1913, 1920 (Fed. Cir. 1989). Finally, "[t]he elements must be arranged as required by the claim." § 2131 (8th ed., 2001), p. 2100-69.

Applicants respectfully traverse the Examiner's rejection of claims 1-6, 9-11, and 17-18 under 35 U.S.C. § 102(e) as being anticipated by Dworkin et al., because each and every element of the claims in issue are not found in a single reference. For example, claim 2, as amended herein, provides for an arithmetic apparatus incorporated in a LSI for performing a long integer product-sum arithmetic operation, the arithmetic apparatus comprising: an integer based unit arithmetic circuit; a finite field GF(2^m) based unit arithmetic circuit logically adjacent to said integer based unit arithmetic circuit; and a selector configured to select one of said integer unit arithmetic circuit and said finite field GF(2^m) based unit arithmetic circuit.

Dworkin et al. discloses an arithmetic processor including a finite field unit 34, an integer modular arithmetic unit 36, and a mode selection control 10 for selectively enabling either the finite field computations or modular integer computations. In contrast, systems and methods consistent with the present invention as recited for example in claim 2, provide an integer based unit arithmetic circuit, a finite field GF(2^m) based unit arithmetic circuit, and a selector for selecting between the two circuits, all *incorporated in an LSI*. Dworkin et al. does not disclose incorporating an integer based unit arithmetic circuit, a finite field GF(2^m) based unit arithmetic circuit, and a selector on an LSI.

For at least the foregoing reasons, Applicants submit that claim 2 is not anticipated by Dworkin et al. Because claim 6 is an independent claim with limitations similar to those of claim 2, Applicants further submit that claim 6 is not anticipated by Dworkin et al. for at least the reasons given with respect to claim 2.

Claim 11, as presented herein, provides for an arithmetic apparatus incorporated in a LSI, comprising: an arithmetic unit module including a long product-sum operation circuit which executes a modular multiplication with a finite field GF(2^m) based polynomial base expression; and a controller module configured to divide the modular multiplication into multiply processing and a modulo and causing said long product-sum operation circuit to execute the modular multiplication.

Applicants respectfully submit that Dworkin et al. does not disclose this claimed combination of elements. Among other things, the cited reference does not disclose at least "a controller module configured to divide the modular multiplication into multiply processing and a modulo and causing said long product-sum operation circuit to execute the modular multiplication" as claimed.

In rejecting claim 11, the Examiner alleged that Dworkin et al. discloses "'computing A*B mod M' wherein the circuit directs A to be multiplied by B and the result [is] computed modulus M (see col. 10, lines 18-30)." This section of Dworkin et al., however, does not teach a *controller module* configured to divide a modular multiplication into multiply processing and a modulo and *causing a long product-sum* *operation circuit* to execute the modular multiplication as claimed. Additionally, no other portions of Dworkin et al. teach or suggest such a feature.

Accordingly, Dworkin et al. does not disclose, teach, or suggest at least "a controller module configured to divide the modular multiplication into multiply processing and a modulo and causing said long product-sum operation circuit to execute the modular multiplication" as claimed. Moreover, Dworkin et al. does not disclose at least an arithmetic unit module and a controller module as part of an arithmetic apparatus *incorporated in an LSI* as claimed.

For at least the foregoing reasons, Applicants submit that claim 11 is not anticipated by Dworkin et al.

The dependent claims 3-5, 7-10, 12, and 17-18 are allowable not only for the reasons stated above with regard to their respective allowable base claims, but also for their own additional features that distinguish them from Dworkin et al.

The Examiner rejected claim 13 under 35 U.S.C. § 103(a) as being unpatentable over Dworkin et al. in view of Carroll et al. Because claim 13 is a dependent claim, the rejection of this claim is unsupportable for the reasons stated above with regard to its respective allowable base claim. Moreover, Applicants respectfully submit that this claim is distinguishable over the applied references for its own patentable features.

The Examiner rejected claims 14-15 under 35 U.S.C. § 103(a) as being unpatentable over Dworkin et al. in view of Carroll et al., and in further view of Zook. Because claims 14-15 are dependent claims, the rejection of these claims are unsupportable for the reasons stated above with regard to their respective allowable

[redacted]

base claims. Moreover, Applicants respectfully submit that these claims are distinguishable over the applied references for their own patentable features.

Moreover, Applicants point out that the rejection to the claims omits any rejections of claims 7 and 8. Any attempt to finalize a rejection of claims 7 and 8 in the next Office Action by the Examiner, if the same should be made final, would be improper.

The Examiner indicated that claim 16 would be allowable if rewritten in independent form. New claim 19 corresponds to claim 16 rewritten in independent form. Accordingly, because new claim 19 corresponds to a claim indicated as allowable if rewritten in independent form, claim 19 is allowable.

Since each of the claims is allowable, Applicants respectfully request the timely allowance of this application.

If an extension of time under 37 C.F.R. § 1.136 is required to obtain entry of this Amendment, such extension is requested. If there are any other fees due under 37 C.F.R. §§ 1.16 or 1.17 which are not enclosed herewith, including any fees required for an extension of time under 37 C.F.R. § 1.136, please charge such fees to our Deposit Account No. 06-0916.

Respectfully submitted,

FINNEGAN, HENDERSON, FARABOW,
GARRETT & DUNNER, L.L.P.

Dated: March 30, 2004

By:____________________
Walter D. Davis, Jr.
Reg. No. 45,137